IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Robert STONER *et al.*	Confirmation No.: 3775
Filed: December 3, 2003	Group Art Unit: 2179
Customer No.: 25537	Examiner: Tran, M.
Attorney Docket: COS97083C1	

For: ALARM MONITORING SYSTEM FOR A TELECOMMUNICATIONS NETWORK

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated May 2, 2008.

I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wireless, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

II. RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III. STATUS OF THE CLAIMS

Claims 1-38 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-38 on January 3, 2008.

IV. STATUS OF AMENDMENTS

No amendments have been made to the claims.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The claimed invention addresses problems associated with network alarm monitoring systems. Prior art network alarm monitoring systems were not easily configurable; and this prevented a user from easily specifying the types of messages that should be designated as alarms and which actions should be taken on each type of message. Moreover, prior art network alarm monitoring products were not designed to be open and portable for use in different platforms.

The claimed invention provides a greater degree of configuration and reliability than the prior art systems by allowing clients to monitor and to log onto systems, and to create and configure text-based rules for monitoring alarms, specifying the actions to be taken on which messages.

Independent claim 1 provides for the following:

1. In a communications network having one or more network elements capable of generating various messages having attributes indicating the existence of an alarm condition (See,

e.g., Specification, page 4, lines 1-31; Fig. 2), an apparatus for remotely monitoring alarm messages comprising:

first means for receiving communication of original textual messages generated from one or more network element subsystems the network element subsystems including console connections and application connections (See, e.g., Specification, page 7, lines 15-31; Fig. 2, elements 81-84, 99);

means for mapping text of a received original message to one or more of a plurality of alarm attributes (See, e.g., Specification, page 7, lines 29-31, page 10, lines 1-5, page 20, line 18-page 21, line 26; Fig. 4, element 63, Fig. 5);

means for determining the presence of an alarm condition from said one or more attributes and generating one or more responses according to said type of alarm condition (See, e.g., Specification, page 11, line 15-page 20, line 17; Fig. 4); and,

means for enabling a remotely located user access to said one or more network elements via a display interface (See, e.g., Specification, page 22, line 32; Fig. 7, element 105) at a remote terminal (See, e.g., Specification, page 21, line 34; Figs. 6a, 6b, element 60), said response including automatically presenting said remotely located user of an alarm condition at a network element via said display interface, said remotely located user being enabled to access said network element from said remote terminal for further responsive action thereof (See, e.g., Specification, page 21, line 32-25, line 2; Figs. 6a, 6b, 7).

Independent claim 21 provides for the following:

21. In a communications network having one or more network elements capable of generating various messages having attributes indicating the existence of an alarm condition, a method for remotely monitoring alarm messages comprising:

receiving communication of original textual messages generated from one or more network element subsystems the network element subsystems including console connections and application connections (See, e.g., Specification, page 7, lines 15-31; Fig. 2, elements 81-84, 99);

mapping text of a received original message to one or more of a plurality of alarm attributes (See, e.g., Specification, page 7, lines 29-31, page 10, lines 1-5, page 20, line 18-page 21, line 26; Fig. 4, element 63, Fig. 5);

determining the presence of an alarm condition from said one or more attributes and generating one or more responses according to said type of alarm condition (See, e.g., Specification, page 11, line 15-page 20, line 17; Fig. 4); and,

enabling a remotely located user access to said one or more network elements via a display interface (See, e.g., Specification, page 22, line 32; Fig. 7, element 105), wherein a response includes automatically presenting said remotely located user of an alarm condition via said display interface, said remotely located user (See, e.g., Specification, page 21, line 34; Figs. 6a, 6b, element 60) capable of accessing said particular network element generating said alarm condition for further responsive action thereof (See, e.g., Specification, page 21, line 32-25, line 2; Figs. 6a, 6b, 7).

Independent claim 36 provides for the following:

36. A telecommunications network alarm monitoring system comprising: a service control point comprising:

a transaction server (See, e.g., Specification, page 6, lines 4 and 12, Fig. 2, element 75);

a communications server (See, e.g., Specification, page 6, lines 4 and 13, Fig. 2, element 76); and

a terminal server to provide access to a plurality of event messages from the transaction server and communications server and to transmit the same over a network link (See, e.g., Specification, page 6, lines 28-30, page 7, lines 1-13; Fig. 2, elements 80a, 80b);

a telecommunications network alarm monitoring server linked to the terminal server of the service control point over the network link (See, e.g., Specification, page 6, lines 12-34, page 7, lines 32-34, page 8, line 1-page 10, line 8; Fig. 2, elements 50, 55a, 55b, 57a, 57b);

a network alarm monitoring process to map the event messages to an alarm data structure (See, e.g., Specification, page 7, lines 29-31, page 10, lines 9-22, Fig. 4, element 63, Fig. 5); and

a network link to the telecommunications network alarm monitoring server to enable transmission of messages by the network alarm monitoring server in response to recognized alarm conditions (See, e.g., Specification, page 8, lines 17-page 10, line 8; Fig. 2, element 92).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-38 are anticipated under 35 U.S.C § 102(b) by *Dev et al.* (US 5,504,921)?

VII. ARGUMENT

A. CLAIMS 1-38 ARE NOT ANTICIPATED OVER *DEV ET AL.*, BECAUSE *DEV ET AL.* FAILS TO DISCLOSE THE CLAIMED FEATURE OF "THE NETWORK ELEMENT SUBSYSTEMS INCLUDING CONSOLE CONNECTIONS AND APPLICATION CONNECTIONS."

The Examiner contends that *Dev et al.* discloses console connections and application connections by arguing "the network portions in buildings 42 and 48 being interconnected by a bridge 50. A building 52 remotely located from buildings 42 and 48 contains network devices 53, 54, 55 and 56 are interconnected by a data bus 57. The network device in building 52 are interconnected to the network in building 48 by interface devices 59 and 60 which may communicated by a packet switching system, a microwave link or a satellite link..." [sic] (Advisory Action of March 27, 2008-paragraph 11). The Examiner concludes that *Dev et al.* "clearly teaches that messages are generated by console connection and application connections because the system teaches a telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system."

Respectfully, the Examiner's rationale is based on speculation, as no console connections and application connections have been identified in *Dev et al.* by the Examiner, nor can they be identified because *Dev et al.* discloses no such connections.

Appellants would point out that the rejection of claims 1-38 is based on anticipation under 35 U.S.C. §102. A rejection for anticipation under section 102 requires that the four corners of a single prior art document describe every element of the claimed invention, either expressly or inherently, such that a person of ordinary skill in the art could practice the invention without undue experimentation. *See Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383, 58

USPQ2d 1286, 1291 (Fed. Cir. 2001); *Atlas Powder Co. v. Ireco Inc.,* 190 F.3d 1342, 1347, 51 USPQ2d 1943, 1947 (Fed. Cir. 1999); *In re Paulsen*, 30 F.3d 1475, 1478-79, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994); *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991).

In general terms, "console connections and application connections" (without the context of the claims) may be known. This general proposition may be why the Examiner has been unyielding in insisting that there must be such connections within the system of *Dev et al.* However, even if known, the claims do not simply recite in general "console connections and application connections. " In order for the prior art to meet the claimed feature, these "console connections and application connections" must be taught in the context of the instant claims. That is, taking claim 1 for example, there must be shown, in the applied reference, a "first means for receiving communication of original textual messages generated from one or more network element subsystems the network element subsystems including console connections and application connections." Thus, it is the network element subsystems that generate the original textual messages that include "console connections and application connections."

Moreover, there is no **express** disclosure of console connections and application connections in *Dev et al.* As such, the Examiner appears to be relying on inherency for a teaching of these claimed elements within the *Dev et al.* system. However, inherency may not be established by probabilities or possibilities. *In re Oelrich,* 666 F.2d 578, 581, 212 USPQ 323, 326 (CCPA 1981). A prior art reference anticipates a patent claims if it discloses every limitation of the claimed invention, either explicitly **or inherently**. *In re Schreiber*, 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1431 (Fed. Cir. 1997). "Under the principles of inherency, if the prior art necessarily functions in accordance with, or includes, the claimed limitations, it anticipates."

MEHL/Biophile Int'l Corp. v. Milgraum, 192 F.3d 1362, 1365, 52 USPQ2d 1303, 1305 (Fed. Cir. 1999).

In order for such console connections and application connections to be inherent in *Dev et al.*, these connections must, **necessarily**, be there. Of course, even if such connections **could** be applicable to the system of *Dev et al.*, they are not **necessarily** required for the system of *Dev et al.* to operate. Accordingly, **the claimed console connections and application connections are neither expressly nor inherently disclosed by *Dev et al.*** and, therefore, the instant claimed subject matter on appeal cannot be anticipated by *Dev et al.*

B. THE REFERENCE TO *DEV ET AL.* FAILS TO DISCLOSE THE CLAIMED FEATURE OF "MEANS FOR MAPPING TEXT OF A RECEIVED ORIGINAL MESSAGE TO ONE OR MORE OF A PLURALITY OF ALARM ATTRIBUTES."

Independent claim 1 recites, *inter alia*, "means for **mapping text** of a received original message **to one or more of a plurality of alarm attributes**." Independent claim 21 recites, *inter alia*, "**mapping text** of a received original message **to one or more of a plurality of alarm attributes**." Independent claim 36 recites, *inter alia*, "a network alarm monitoring process to **map the event messages to an alarm data structure**."

The Examiner indicated in the Final Office Action of January 3, 2008, at page 3, that the "mapping text" feature is to be found at col. 4, lines 54-65, and col. 12, lines 32-50, of *Dev et al.* However, there is no teaching of the claimed mapping at the cited portion of column 4, as this relates only to servicing user requests and providing network information, e.g., alarms, to a user interface. With regard to the cited portion of column 12, the only reference to a "map" in this section of the reference relates to a "map 300 of the northeast region," indicative of a geographical map, and not a mapping of text of an original message to one or more of a plurality

of alarm attributes. Moreover, to the extent that there is any mapping to alarm attributes disclosed by *Dev et al.*, an assumption with which Appellants do not agree, there is no mapping of **text** of a received original message to one or more of a plurality of alarm attributes.

Appellants again note that the rejection is based on anticipation under 35 U.S.C. §102. As such, the Examiner should be able, and, in fact, is required, to point to something specific within the disclosure of *Dev et al.* that serves the function of mapping text of a message to one or more of a plurality of alarm attributes. However, the Examiner has not done so. Instead, the Examiner resorts to attacking the language of the claim, i.e., "mapping text…" as "a broad term." But if the "mapping" language of the claims is as broad as the Examiner alleges, the Examiner should be able to explain how this term is being interpreted within the context of the reference. The Examiner does not provide any explanation, preferring instead to identify two seemingly irrelevant portions of the reference and to leave Appellants to speculate as to what meaning the Examiner is giving to the claim language.

As the Honorable Board is well aware, rudimentary patent examination rules and the patent statute (under 35 U.S.C. §102, a person "**shall be** entitled to a patent **unless**…") place the initial burden on the Examiner, and not on the Applicant, to present a *prima facie* case of anticipation before the Applicant is required to argue for patentability. The Examiner has not presented such a *prima facie* case.

With regard to the Examiner's allegation that the "mapping" language is "not specific and clear enough…," (Final Office Action of January 3, 2008-page 8), this is irrelevant to a rejection under 35 U.S.C. §102. If the language is not specific or clear enough, the rejection should have been under 35 U.S.C. §112, second paragraph, and not under 35 U.S.C. §102. *Cf. In re Steele*, 305 F.2d 859, 134 USPQ 292 (CCPA 1962). However, the claim language is very specific. It

clearly calls for the mapping of text of a received message to one or more of a plurality of alarm attributes.

The rejection of claims 1-38 must be reversed, because *Dev et al.* does not disclose the features of the claims, and, accordingly, the Honorable Board is respectfully requested to reverse the rejection of claims 1-38 under 35 U.S.C. §102(b).

VIII. CONCLUSION AND PRAYER FOR RELIEF

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the Examiner's rejections.

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 504213 and please credit any excess fees to such deposit account.

Respectfully Submitted,

DITTHAVONG MORI & STEINER, P.C.

January 8, 2009
Date

/Phouphanomketh Ditthavong/
Phouphanomketh Ditthavong
Attorney for Applicant(s)
Reg. No. 44658

Errol A. Krass
Attorney for Applicant(s)
Reg. No. 60090

918 Prince Street
Alexandria, VA 22314
Tel. 703-519-9952
Fax. 703-519-9958

IX. CLAIMS APPENDIX

1. In a communications network having one or more network elements capable of generating various messages having attributes indicating the existence of an alarm condition, an apparatus for remotely monitoring alarm messages comprising:

first means for receiving communication of original textual messages generated from one or more network element subsystems the network element subsystems including console connections and application connections; means for mapping text of a received original message to one or more of a plurality of alarm attributes;

means for determining the presence of an alarm condition from said one or more attributes and generating one or more responses according to said type of alarm condition; and,

means for enabling a remotely located user access to said one or more network elements via a display interface at a remote terminal, said response including automatically presenting said remotely located user of an alarm condition at a network element via said display interface, said remotely located user being enabled to access said network element from said remote terminal for further responsive action thereof.

2. The apparatus as claimed in claim 1, wherein said first server means includes a terminal server means physically connected to a console port I/O of each said network element, said remotely located user having access to said console port via said user interface.

3. The apparatus as claimed in claim 1, wherein said first server means includes means for receiving communication of original textual messages from a network application running on said network element, said first server means including a mailbox facility means for receiving said

alarm messages.

4. The apparatus as claimed in claim 1, wherein said network application running on said network element is a Log Management Facility application.

5. The apparatus as claimed in claim 1, further comprising means for presenting an indication of said alarm condition to said remotely located user via a network connection.

6. The apparatus as claimed in claim 5 wherein said indication of said alarm condition is presented as on said display interface as a graphical icon, said graphical icon being color-coded to indicate alarm condition severity.

7. The apparatus as claimed in claim 2, wherein said terminal server means includes a telnet terminal server.

8. The apparatus as claimed in claim 7, wherein said means for enabling a remotely located user access to said one or more network elements includes a network connection.

9. The apparatus as claimed in claim 7, wherein said network socket connection is pursuant to a TCP/IP protocol.

10. The apparatus as claimed in claim 1, wherein said means for mapping text of a received original message to one or more of a plurality of alarm attributes includes utilizing regular

expression matching.

11. The apparatus as claimed Mi claim 1, wherein said message attributes include one or more selected from the group comprising: originating network element, time, alarm severity level, alarm mnemonic, alarm description, process name, and network element name.

12. The apparatus as claimed in claim 11, wherein said means for determining presence of an alarm condition from said one or more attributes includes means for applying configuration rules to said alarm attributes, said configuration rules stored as text in a first storage means at or near said first means and accessible therefrom.

13. The apparatus as claimed in claim 12, further including text editor means for enabling a user to modify existing configuration rules stored in said storage means via said user display interface, said text editor means further enabling said user to generate new configuration rules for storage in said storage means, said new configuration rules creating a new alarm condition.

14. The apparatus as claimed in claim 12, wherein said configuration rules further provides a sifting operation for sifting through said attributes to match said alarm condition with a pre-determined alarm condition.

15. The apparatus as claimed in claim 14, wherein said sifting means operation enables an alarm message to be terminated if a match with a pre-determined alarm condition is found.

16. The apparatus as claimed in claim 12, wherein said configuration rules further provide a logging operation for automatically logging alarm conditions in a second storage means at or near said first means and accessible therefrom.

17. The apparatus as claimed in claim 16, further including means for generating reports including past alarm conditions stored in said second storage means.

18. The apparatus as claimed in claim 1, wherein a response action includes initiating transmission of an e-mail message and command procedure.

19. The apparatus as claimed in claim 1, wherein a response action includes initiating transmission of a paging message and command procedure.

20. The apparatus as claimed in claim 1, wherein said physical connection to said console port I/O includes an RS-232 link.

21. In a communications network having one or more network elements capable of generating various messages having attributes indicating the existence of an alarm condition, a method for remotely monitoring alarm messages comprising:

receiving communication of original textual messages generated from one or more network element subsystems the network element subsystems including console connections and application connections;

mapping text of a received original message to one or more of a plurality of alarm attributes;

determining the presence of an alarm condition from said one or more attributes and generating one or more responses according to said type of alarm condition; and,

enabling a remotely located user access to said one or more network elements via a display interface, wherein a response includes automatically presenting said remotely located user of an alarm condition via said display interface, said remotely located user capable of accessing said particular network element generating said alarm condition for further responsive action thereof.

22. The method as claimed in claim 21, further including providing a physical connection between each said network element and a terminal server device enabling remote access to said one or more network elements via said user display interface.

23. The method as claimed in claim 21, further including providing a mailbox facility means for receiving said alarm messages, and retrieving said messages from said mailbox facility prior to said mapping step.

24. The method as claimed in claim 21, further including providing a network connection to enable presentation of said alarm condition to said remotely located user, said alarm condition being presented on said display interface as a graphical icon.

25. The method as claimed in claim 24, wherein said graphical icon is color-coded to indicate

alarm condition severity.

26. The method as claimed in claim 21, further including providing a network socket connection to enable said remotely located user access to said one or more network elements.

27. The method as claimed in claim 26, wherein said network socket connection is pursuant to a TCP/IP protocol.

28. The method as claimed in claim 21, wherein said step of mapping text includes utilizing regular expression matching.

29. The method as claimed in claim 21, wherein said message attributes include one or more selected from the group comprising: originating network element, time, alarm severity level, alarm mnemonic, alarm description, process name, and, network element name.

30. The method as claimed in claim 21, wherein said determining step includes applying configuration rules to said alarm attributes, said configuration rules being stored as text in a first storage means at or near said first means and accessible therefrom.

31. The method as claimed in claim 30, further providing text editor means for enabling a user to modify existing configuration rules stored in said storage means via said user display interface, said text editor means further enabling said user to generate new configuration rules for storage in said first storage means, said new configuration rules creating a new alarm condition.

32. The method as claimed in claim 30, wherein said step of applying configuration rules further includes performing a sifting operation for sifting through said attributes to match said alarm condition with a pre-determined alarm condition.

33. The method as claimed in claim 32, wherein said sifting operation enables an alarm message to be terminated if a match with a pre-determined alarm condition is found.

34. The method as claimed in claim 30, wherein said step of applying configuration rules further includes the step of performing a logging operation for automatically logging alarm conditions in a second storage means at or near said first storage means and accessible therefrom.

35. The method as claimed in claim 34, further including the steps of accessing alarm condition stored in said second storage means and generating reports containing said past alarm conditions.

36. A telecommunications network alarm monitoring system comprising: a service control point comprising:

a transaction server;

a communications server; and

a terminal server to provide access to a plurality of event messages from the transaction server and communications server and to transmit the same over a network link;

a telecommunications network alarm monitoring server linked to the terminal server of the service control point over the network link;

a network alarm monitoring process to map the event messages to an alarm data structure; and

a network link to the telecommunications network alarm monitoring server to enable transmission of messages by the network alarm monitoring server in response to recognized alarm conditions.

37. The telecommunications alarm monitoring system of claim 36 wherein access is enabled to the terminal server is over an Internet Protocol network.

38. The telecommunications alarm monitoring system of claim 36 wherein the link to the telecommunications network alarm monitoring server to enable transmission of messages by the telecommunications network alarm monitoring server in response to recognized alarm conditions comprises an Internet Protocol network.

X. EVIDENCE APPENDIX

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI. RELATED PROCEEDINGS APPENDIX

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.